EXHIBIT A

DoD Manual 5200.08 VOLUME 3

PHYSICAL SECURITY PROGRAM: ACCESS TO DOD INSTALLATIONS

Originating Component:	Office of the Under Secretary of Defense for Intelligence and Security
Effective:	January 2, 2019
Change 1 Effective:	September 18, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Incorporates and Cancels:	Directive Type Memorandum 09-012, "Interim Policy Guidance for DoD Physical Access Control," December 8, 2009
Approved by:	Joseph D. Kernan, Under Secretary of Defense for Intelligence
Change 1 (Administrative) Approved by:	Christopher R. Choate, Chief, Directives Division

Purpose: This manual is composed of several volumes, each containing its own purpose. In accordance with DoD Directive (DoDD) 5143.01 and DoD Instruction (DoDI) 5200.08:

- The manual implements policy, assigns responsibilities, and prescribes procedures for managing and executing the DoD Physical Security Program.
- This volume assigns responsibilities and prescribes procedures for controlling physical access to DoD installations consistent with Section 1069 of Public Law 110-181 and Section 1086 of Public Law 114-92 by establishing:
  - Standards and methods for verifying the identity of and protocols for determining the fitness of individuals entering DoD installations.

- Three types of access to DoD installations: unescorted, trusted traveler, and escorted.
- Three types of installations for the purposes of controlling access to DoD installations: electronic physical access control system (ePACS)-enabled DoD installations with Identity Matching Engine for Security and Analysis (IMESA) functionality, ePACS-enabled DoD installations without IMESA functionality, and non-ePACS-enabled DoD installations.

- This volume supersedes any conflicting portion of DoD 5200.08-R pertaining to installation access and emergency planning.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION 4
1.1. Applicability. 4
1.2. Policy. 4
1.3. Summary of Change 1. 5
SECTION 2: RESPONSIBILITIES 6
2.1. Under Secretary of Defense for Intelligence and Security (USD(I&S)). 6
2.2. Director, Defense Intelligence Agency (DIA). 6
2.3. USD(P&R). 6
2.4. DoD Component Heads With Authority, Direction or Control Over Installations. 7
SECTION 3: REQUIREMENTS FOR ACCESS TO A DOD INSTALLATION 9
3.1. Requirements Based on Type of Access. 9
3.2. Establishing Identity For Unescorted Access. 9
3.3. Establishing Fitness For Unescorted Access. 10
3.4. Establishing Purpose For Access. 12
3.5. Requirements For Special Events and Emergencies. 13
3.6. Related Measures. 13
3.7. Additional Requirements. 14
SECTION 4: PROCEDURES FOR GRANTING ACCESS TO A DOD INSTALLATION 15
4.1. Granting Escorted Access. 15
4.2. Granting Trusted Traveler Access. 15
4.3. Granting Unescorted Access. 17
4.4. VCP. 17
4.5. Enrollment. 19
4.6. Access Control Process. 21
4.7. Automatic Enrollment at the ACP. 22
4.8. ePACS Failure Contingencies. 23
SECTION 5: ACCEPTABLE FORMS OF IDENTIFICATION 24
5.1. Acceptable Credentials. 24
5.2. Source Identity Documents. 27
5.3. Verification Of Credentials. 28
SECTION 6: IMPLEMENTATION 30
6.1. Component Implementing Policies. 30
6.2. Allowable Deviations. 31
6.3. Component Policy for Acceptable Purposes. 31
GLOSSARY 32
G.1. Acronyms. 32
G.2. Definitions. 33
REFERENCES 36

TABLES

Table 1. Summary of Credential Acceptability, Enrollability, and Requirements Established 26
Table 2. Verification Method by Credential and Type of Installation 28
Table 3. Verification Methods 29

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance applies to:

(1) The Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within DoD (referred to collectively in this issuance as the "DoD Components").

(2) The **grounds** of DoD installations and facilities on DoD-owned or DoD-leased land that have a perimeter barrier (such as a fenceline or wall), access control point (ACP), and a method for processing visitors (collectively referred to as "installations"). Heads of DoD Components may extend applicability to the grounds of facilities under their authority, direction, and control, including grounds of DoD installations without a perimeter barrier, ACP, or method for processing visitors, or any portion of grounds outside the United States if permitted by applicable host-nation agreements, status of forces agreements, or other requirements.

(3) DoD installations located within the United States (including the continental United States, Alaska, Hawaii, Puerto Rico, and Guam). Heads of DoD Components may extend applicability to installations in foreign countries if permitted by applicable host-nation agreements, status of forces agreements, or other requirements.

b. This issuance does **not** apply to:

(1) Individual buildings on or off DoD installations.

(2) Space in leased buildings or leased offices; space managed and operated by other federal agencies; or contractor facilities.

(3) Installations, or portions of installations, that house non-DoD facilities exclusively.

1.2. POLICY.

It is DoD policy that:

a. In accordance with DoDI 5200.08, DoD installations, property, and personnel must be protected. Commanders have authority to take reasonably necessary and lawful measures to protect installation property and personnel, but that authority must not be exercised in an arbitrary, unpredictable, or discriminatory manner. Removal or denial actions must be based on reasonable grounds and be judiciously applied.

b. In accordance with DoDI 5400.11, personally identifiable information collected, used, maintained, or disseminated in the execution of this issuance will be appropriately maintained and safeguarded to prevent its unauthorized access, use, disclosure, or loss. The collection, use, maintenance, and dissemination of personally identifiable information must comply with the

requirements of 5 U.S.C. 552a, DoDD 5200.27, DoDI 5400.11, DoD 5400.11-R, DoDI 5505.17, DoDI 5400.16, and Volume 4 of DoD Manual (DoDM) 5200.01.

1.3. SUMMARY OF CHANGE 1. This administrative change updates:

a. The title of the Under Secretary of Defense for Intelligence to the Under Secretary of Defense for Intelligence and Security in accordance with Public Law 116-92.

b. Administrative changes in accordance with current standards of the Office of the Chief Management Officer of the Department of Defense.

SECTION 2: RESPONSIBILITIES

2.1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (USD(I&S)). The USD(I&S):

a. Establishes physical security access control standards, procedures, and guidance consistent with this issuance, DoDD 5143.01, DoDI 5200.08, approved federal standards, and applicable laws.

b. Coordinates with the Under Secretary of Defense for Acquisition and Sustainment and the Under Secretary of Defense for Personnel and Readiness (USD(P&R)):

(1) To provide oversight of the development of interfaces associated with controlling physical access.

(2) To develop technical and interface requirements for identification card issuance, revocation notification, and system interoperability with ePACSs.

c. Identifies authoritative government databases required for initial checks to establish historic fitness and for recurring checks to maintain current fitness, as described in Section 3.

d. Establishes processes for establishing the identity of individuals seeking access, as described in Section 5, by verifying credentials and verifying the cardholder is the individual to whom the credential was issued.

e. Reviews and adjudicates requests for un-manned vehicular access points, as described in Section 4.

2.2. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). Under the authority, direction, and control of the USD(I&S), and in addition to the responsibilities in Paragraph 2.4, the Director, DIA, provides threat information required for risk assessments by DoD Component heads and installation commanders.

2.3. USD(P&R). The USD(P&R):

a. Designs and maintains the IMESA, the Interoperability Layer Service (IoLS), successor, and other systems necessary to implement this issuance.

b. Ensures such systems are designed and maintained in compliance with applicable law, federal regulations, and DoD policy including, but not limited to:

(1) Section 552a of Title 5, United States Code (U.S.C.); and Chapter 35, Subchapter I of Title 44, U.S.C., regarding the collection and retention of information on and from U.S. citizens.

(2) DoDD 5200.27 regarding the acquisition of information on persons not affiliated with DoD.

c. Establishes, and, as funds are available for such purposes, executes a plan to integrate IMESA with ePACS at all DoD installations.

d. Coordinates with the USD(I&S) and the DoD Component heads, as appropriate, regarding the authoritative government databases that such systems shall check for historic and current fitness and other applicable reporting requirements.

2.4. DOD COMPONENT HEADS WITH AUTHORITY, DIRECTION OR CONTROL OVER INSTALLATIONS. DoD Component heads with authority, direction, or control over installations:

a. Establish DoD Component-level policies for installation access control that contain, at a minimum, the items listed in Paragraph 6.1.

b. Implement procedures for all populations to gain access to component installations.

(1) Such procedures will establish a uniform process to establish identity, fitness, and purpose for gaining access to component installations and be implemented consistently and predictably.

(2) All other physical security measures are subject to randomization and unpredictability requirements for security purposes, but shall not be arbitrary or discriminatory.

c. Field ePACS at all component installations.

(1) New ePACS and ePACS undergoing significant upgrade (valued at more than 50 percent of replacement cost) must interface with IMESA via the IoLS and read, enroll, and electronically verify all listed credentials as described in Section 5.

(2) All ePACS must comply with 5 U.S.C. 552a, DoDI 8910.01, DoDI 5400.16, DoDI 5400.11, and DoD 5400.11-R.

d. Implement at all component installations:

(1) A training program for perimeter security personnel, including at both the ACP and visitor control center (VCC), on the requirements, processes, and prohibitions described in this issuance and the appropriate DoD Component policy.

(2) A redress and appeal process for individuals denied unescorted access.

(3) Credential requirements, fitness disqualifications, Privacy Act statement, and redress and appeal processes, ensuring they are clearly and conspicuously posted at the VCC and on the installation website if one exists.

(4) A determination of the acceptable purposes for accessing the installation, in accordance with this volume, applicable Federal, State and local laws, DoD policy, and DoD Component policies.

(5) Coordination with local first responders to establish appropriate standard operating procedures for facilitating access to first responders during emergencies, in accordance with Paragraph 3.5 of this issuance.

(6) Alternate means to process visitors through the visitor control process (VCP) when the VCC is closed.

e. Adjudicate requests for deviations listed in Section 6 for installations under their authority, direction, and control, and review each approved deviation annually to assess associated risks. The only allowable deviations are listed in Section 6.

(1) DoD Component heads will notify the Office of the USD(I&S) Director of Counterintelligence and Security within 30 days of approved deviations.

(2) Requests and approvals must address any residual risks associated with the deviations.

f. May delegate the approval authority for deviations listed in Section 6 only to one of the following officials within their respective Departments:

(1) Within the Department of the Navy, to the Under Secretary of the Navy, to the Chief of Naval Operations, or to the Commandant of the Marine Corps.

(2) Within the Department of the Army, to the Under Secretary of the Army or to the Chief of Staff of the Army.

(3) Within the Department of the Air Force, to the Under Secretary of the Air Force or to the Chief of Staff of the Air Force.

(4) Within the Defense Logistics Agency, to the Deputy Director of the Defense Logistics Agency.

g. Fund the operation, maintenance, and enhancement of IMESA with additional government data sources.

SECTION 3: REQUIREMENTS FOR ACCESS TO A DOD INSTALLATION

3.1. REQUIREMENTS BASED ON TYPE OF ACCESS. There are three types of access to a DoD installation: unescorted, trusted traveler and escorted. Each type of access has a specific set of requirements which must be implemented consistently, uniformly, and predictably to facilitate entry by authorized personnel.

a. Unescorted Access. Unescorted access requires individuals to establish their identity, be determined fit for access, and establish an acceptable purpose for presence on the installation, except only under the following circumstances:

(1) Special events and emergencies, in accordance with Paragraph 3.5 of this issuance.

(2) Portions of installations consisting of large unoccupied, undeveloped space, if permitted under DoD Component policy. This exception is not considered a deviation.

(3) Installations with a mission that requires open, unimpeded access to the public, when approved as a deviation in accordance with Paragraphs 2.4.e, 2.4.f, and 6.2 of this issuance.

(4) A minor under the age of 18 who does not have an acceptable credential and is accompanied by a parent or guardian who is age 18 or older and who has been granted unescorted access. This exception is not considered a deviation.

b. Trusted Traveler Access. Trusted traveler programs allow authorized individuals who have been granted unescorted access, based on low- or medium-risk verified credentials as defined in Table 3, to simultaneously vouch for co-travelers (in the same vehicle or on foot) and enable those co-travelers to obtain trusted traveler access. Trusted traveler access, if permitted at the installation by this volume and DoD Component and installation-level policy, requires individuals to have an acceptable purpose for their presence on the installation and be capable of establishing their identity and being determined fit for access upon demand by installation security personnel. Individuals may be required to establish their identity in accordance with Paragraph 3.2 based on DoD Component and installation-level policy. .

c. Escorted Access. Individuals unable to meet the identity or fitness requirements for trusted traveler or unescorted access may be granted escorted access, in accordance with DoD Component and installation-level policy. Escorted access requires individuals to establish an acceptable purpose for their presence on the installation.

3.2. ESTABLISHING IDENTITY FOR UNESCORTED ACCESS. Identity is established either by presenting **one** "acceptable credential" or by presenting an acceptable combination of "source identity documents." Acceptable credentials and source identity documents are listed in Section 5 of this issuance.

a. Acceptable credentials and source identity documents must:

(1) Be original and current (unexpired).

(2) Not contain the markings "Not Valid for Federal Purposes," "Not For Use as Federal Identification," "Federal Limits May Apply," or any other similar phrase.

(3) In the case of a driver's license or non-driver's identification card issued by a State, territory, possession, or the District of Columbia, be compliant with the REAL ID Act of 2005.

b. Individuals holding more than one acceptable credential must use the credential most accurately depicting the capacity in which the individual is acting for the specific visit to the installation, in accordance with Volume 1 of DoDM 1000.13.

c. DoD Component heads and installation commanders will not require more than one acceptable credential to establish identity as a standard access control process. Intermittent requirements to present additional credentials as a random antiterrorism measure are considered part of an installation's antiterrorism program, not access control.

d. DoD Component heads and installation commanders will accept all types of credentials listed in Section 5 as acceptable for their type of installation. Installation commanders with unique mission requirements may refuse to accept one or more of the credentials listed in Section 5 as acceptable for their type of installation when approved as a deviation in accordance with Paragraphs 2.4.e, 2.4.f, and 6.2 of this issuance, consistent with applicable laws.

3.3. ESTABLISHING FITNESS FOR UNESCORTED ACCESS. Fitness for access has two elements: historic fitness and current fitness.

a. Historic fitness is established, at a specific point in time, only by means of a review of the individual's prior criminal history through a check of the National Crime Information Center (NCIC), the Interstate Identification Index, and relevant government databases and Service criminal justice information systems. The requirement to establish historic fitness for unescorted access may be met by either:

(1) Establishing historic fitness at the time of access through an on-the-spot review and adjudication conducted by government personnel at an installation or at a centralized processing location.

(2) Proving that historic fitness was previously established by any one of the following:

(a) The acceptable credential used to establish identity, if listed as establishing historic fitness in Section 5 of this issuance;

(b) A previously conducted review and adjudication at an installation if followed, immediately and without lapse, by enrollment in IMESA for continuous vetting;

(c) The DoD Consolidated Adjudication Facility, or predecessor organization, determination that the individual eligible for access to classified information, so long as that eligibility remains in scope;

(d) A favorably adjudicated Tier 1 or higher background investigation performed by the DoD Consolidated Adjudication Facility or other Federal agency that remains in scope; or

(e) Other means established by DoD Component-level policy.

b. Current fitness is established, on a recurring and continuing basis, only through a review (either on-the-spot at the VCC or nightly through IMESA) of an individual's current derogatory information through a check of authoritative government sources (real-time or most recent file from such source). The review includes:

(1) Terrorism lists, such as the NCIC Known and Appropriately Suspected Terrorist file and the Terrorism Screening Database.

(2) Felony wants and warrants, such as those listed in the NCIC Wanted Persons File.

(3) Barment order lists, such as relevant Service criminal justice information systems.

(4) Other relevant government databases that may be available such as:

(a) Other NCIC files (including the National Sex Offender Registry);

(b) Criminal justice or immigration databases; or

(c) Other appropriate biometric or biographic government databases.

c. Until a DoD standard for historic and current fitness is established, DoD Components may establish their own fitness adjudication criteria, subject to the following constraints:

(1) Granting unescorted access to an individual listed on any U.S. Government terrorism watchlist is prohibited, except as provided for in law, executive order, or DoD policy to further counterintelligence or counterterrorism purposes, or in accordance with Annex D to the Memorandum of Understanding between the Federal Bureau of Investigation and the Department of Defense.

(2) Granting unescorted access to an individual with a felony want or warrant is prohibited.

(3) Installation commanders must conspicuously post their established adjudication criteria and redress and appeal process for those negatively adjudicated.

(4) DoD Components may grant unescorted access to a convicted felon, in accordance with applicable Federal, State, and local laws, after considering appropriate mitigating factors such as the nature and seriousness of the offense, the circumstances surrounding the offense, recency and frequency of the offense, the individual's age and maturity at the time of the offense, the individual's effort toward rehabilitation, and other factors.

(5) DoD Components **may** grant unescorted access to individuals **without** U.S. citizenship based on the installation's characteristics or mission. In situations where an

installation requires U.S. citizenship for unescorted access due to characteristics or mission, acceptable proof of citizenship can be demonstrated with any **one** of the following:

(a) An unexpired U.S. passport or passport card.

(b) An original or certified true copy of a birth certificate issued by a State, territory, possession, or the District of Columbia bearing a raised seal.

(c) A certificate of naturalization (Form N-550 or N-570).

(d) A Consular Record of Birth Abroad.

(e) Other documents as established by DoD Component-level policy.

(6) An individual with dual U.S. citizenship will be treated the same as an individual with only U.S. citizenship. Presentation of any one of the documents listed in Paragraph 3.3(c)(5) is sufficient to prove U.S. citizenship.

3.4. ESTABLISHING PURPOSE FOR ACCESS. All individuals must have an acceptable purpose for presence on the installation.

a. Purpose is established by:

(1) The acceptable credential presented if listed as establishing purpose in Section 5.

(2) Documentation including, but not limited to, bills of lading or event tickets. Documentation may be hardcopy or electronic.

(3) Trusted DoD systems such as, but not limited to, the Carrier Appointment System.

(4) Lists including, but not limited to, guest lists, transportation officer delivery/pickup lists, or appointment lists.

(5) Verbal discussion with the individual seeking access.

(6) By other means defined by DoD Component and installation-level policy.

b. Purposes acceptable for access to an installation:

(1) Are defined by DoD Component and installation-level policy.

(2) Will be based on the specific characteristics of each installation.

(3) May vary based on the:

(a) Time of day.

(b) Day of week.

(c) Specific ACP on the installation through which access is being sought.

(d) Current force protection condition at which the installation is operating.

(e) Individual's mission essential or emergency response designation.

(f) Other appropriate factors.

c. Certain purposes may only be valid for specific identities (e.g., a name on appointment list is only a valid purpose if the individual has established their identity, as described in Paragraph 3.2, and that identity matches the entry on the list).

3.5. REQUIREMENTS FOR SPECIAL EVENTS AND EMERGENCIES. After performing a risk assessment, DoD Component heads may grant a temporary waiver to one or more of the requirements outlined in Paragraphs 3.2 and 3.3 of this issuance for special events or in case of an emergency on the installation. DoD Component heads may delegate this authority, in accordance with DoD Component policy, no lower than O-7 or civilian equivalent. Temporary waivers issued under this paragraph are not considered deviations.

a. The requirements must be met to the extent feasible.

b. Installation commanders must manage increased risk associated with waiving these requirements. Measures must be taken to ensure that individuals who have been granted access to the installation for the special event do not have access to other parts of the installation not associated with the event. The special event itself constitutes the acceptable purpose required by paragraph 3.4.

c. Installation commanders will coordinate with local first responder organizations, including law enforcement and fire and medical response organizations, to develop procedures for facilitating access during emergency response events.

(1) Through such procedures, installation commanders may establish appropriate criteria to waive the requirements outlined in Paragraphs 3.2 and 3.3 for first responders to emergency response events. The emergency response event itself constitutes the acceptable purpose required by Paragraph 3.4.

(2) Access control personnel granting access to first responders during an emergency should direct first responders to check in with the on-scene incident commander to coordinate their activities and prevent mistaken identities that could hinder a coordinated response to the emergency.

3.6. RELATED MEASURES. Random antiterrorism measures may be applied in addition to the access control process pursuant to Volumes 1 and 2 of DoDI O-2000.16. DoD Components are authorized to inspect the vehicle, parcels, and belongings of an individual seeking installation access.

3.7. ADDITIONAL REQUIREMENTS. When approved as a deviation in accordance with Paragraphs 2.4.e, 2.4.f, and 6.2, installation commanders with unique mission requirements may establish more restrictive access control requirements. Examples of such situations include, but are not limited to, installations where access requires an active security clearance or very high-profile DoD installations, such as the Pentagon Reservation.

SECTION 4: PROCEDURES FOR GRANTING ACCESS TO A DOD INSTALLATION

4.1. GRANTING ESCORTED ACCESS.

a. Individuals unable to meet the requirements of Paragraphs 3.2 or 3.3 may be granted escorted access to the installation, in accordance with DoD Component and installation-level policies.

b. Escorts must be provided by the organization or individual responsible for sponsoring, or otherwise associated with the individual's visit, and must remain within reasonable visual contact of the individual(s) they are escorting.

c. Escorts must report any conduct by the escorted individual that causes a risk to the safety, security, or efficiency of the installation or its occupants in accordance with installation procedure. Failure to comply with escort duties may result in the temporary or permanent loss of escort privileges.

d. Escorts functioning in their personal capacity or neglectfully functioning in their official capacity may be personally accountable for the conduct of the individual(s) they are escorting in accordance with installation security policies.

e. Escorts must be U.S. citizens, have a DoD affiliation, and themselves be granted unescorted access in accordance with this volume.

f. DoD Component and installation-level policies will determine the number of people an individual may escort and may require specific training or additional qualifications to serve as an escort.

4.2. GRANTING TRUSTED TRAVELER ACCESS.

a. Trusted traveler programs may not be established at non-ePACS-enabled DoD installations, with the sole exception of U.S. uniformed military personnel entering the installation in formation. Procedures for trusted traveler access for uniformed U.S. military personnel in formation will be established by the DoD Component heads.

b. A trusted traveler program may be established by commanders of ePACS-enabled DoD installations, with or without IMESA functionality, in accordance with DoD Component-level policies.

(1) The authorized individual must have sufficient knowledge of the co-travelers to legitimately vouch for their identity, fitness, and purpose. Individuals may be personally accountable for the conduct of those co-travelers in accordance with installation security policies. DoD Component and installation-level policies may require the authorized individual to accompany the co-traveler until he or she departs the installation.

(2) Co-travelers, except uniformed U.S. military personnel co-travelers entering the installation in formation, may be required to establish their identity by presenting an acceptable credential, in accordance with DoD Component and installation-level policies.

(3) DoD Component and installation-level policies will determine the number of co-travelers that an authorized individual may vouch for at any time.

(4) DoD Component and installation-level policies will determine the specific populations of individuals authorized to vouch for co-travelers under the trusted traveler program, except that individuals without both U.S. citizenship and a DoD affiliation are not permitted to do so.

(5) At least one individual must satisfy the requirements outlined in Paragraphs 3.2, 3.3, and 3.4 and be granted unescorted access to be permitted to vouch for co-travelers.

(6) Except as provided for in this volume, procedures for trusted traveler programs are established and implemented locally, and may vary from installation to installation.

(7) Trusted traveler programs are permitted only at force protection conditions NORMAL, ALPHA, and BRAVO, and may be further restricted by the DoD Component head.

(8) Trusted traveler programs must be suspended in the event of an ePACS failure except:

(a) For uniformed military personnel returning in formation.

(b) For the period of time that a suspension would cause a bona fide traffic safety risk, as determined by the installation commander, on a road not owned or managed by DoD.

(c) When doing so would significantly degrade the installation's mission capability as determined, contemporaneously with the ePACS failure, by a commander of at least the grade O-8 and with notification to the Office of the USD(I&S) Director of Counterintelligence and Security within five days. Such determinations may not be made in advance of an ePACS failure or established generally in policy.

(9) In accordance with Component and installation-level policies, when an installation's trusted traveler program is suspended due to an ePACS failure, co-travelers may be:

(a) Granted unescorted access in accordance with Section 4.3 by presenting an acceptable credential listed in Section 5.3 as establishing identity, fitness, and purpose;

(b) Granted escorted access in accordance with Section 4.1 by presenting any acceptable credential; or

(c) Processed through the VCP as a visitor in accordance with Section 4.4.

4.3. GRANTING UNESCORTED ACCESS. DoD Component heads may only grant unescorted access only to individuals who satisfy the unescorted access requirements outlined in Section 3. In addition, with respect to such individuals, DoD Component heads may:

a. Grant **recurring** unescorted access:

(1) To ePACS-enabled DoD installations with IMESA functionality to only those individuals who are currently enrolled in both IMESA and the local installation ePACS.

(2) To ePACS-enabled DoD installations without IMESA functionality to only those individuals who are currently enrolled in the local installation ePACS.

(3) To non-ePACS-enabled DoD installations to only those individuals presenting a DoD Common Access Card (CAC); DoD Uniformed Services Identification card (USID); or Non-CAC Local or Regional DoD Credential (LRC) valid for that particular installation.

b. May grant **short-term** (7 days or less) unescorted access to only those individuals who meet the requirements outlined in Section 3 but do not meet the requirements for recurring unescorted access as described in Paragraph 4.3(a) if such individuals successfully complete the VCP as described in Paragraph 4.4 of this issuance.

c. Process individuals who meet the requirements for recurring unescorted access as described in Paragraph 4.3(a) through the access control process at the ACP, in accordance with Paragraph 4.6 of this issuance.

d. Process individuals who do not meet the requirements for recurring unescorted access as described in Paragraph 4.3(a) through:

(1) Automatic enrollment in accordance with Paragraph 4.7, if eligible; or

(2) The VCP at the VCC in accordance with Paragraph 4.4 of this issuance.

e. May conduct the VCP at the ACP rather than the VCC as long as doing so does not adversely impact the throughput of the ACP or the safety of the ACP personnel. The VCP at the ACP must be the functional equivalent to the VCP at the VCC.

4.4. VCP.

a. Visitors. Visitors are defined based on the type of installation:

(1) At ePACS-enabled DoD installations with IMESA functionality, a visitor is any individual who is not eligible for automatic enrollment under Paragraph 4.7 and:

(a) Is not enrolled in IMESA **and** the local installation ePACS; or

(b) Whose enrollment in IMESA **or** the local installation ePACS has expired.

(2) At ePACS-enabled DoD installations without IMESA functionality, a visitor is any individual who is not eligible for automatic enrollment under Paragraph 4.7 and:

(a) Is not enrolled in the local installation ePACS; or

(b) Whose enrollment in the local installation ePACS has expired.

(3) At non-ePACS-enabled DoD installations, a visitor is any individual who does not hold a CAC, USID, or non-CAC LRC issued by the local installation or region.

b. VCP Procedures. DoD Components will establish VCP procedures.

(1) Such VCP procedures must satisfy all the requirements outlined in Section 3 by:

(a) Establishing identity, using either an acceptable credential or an acceptable combination of source identity documents as described in Section 5.

(b) Establishing historic fitness, either by performing an on-the-spot review as described in Paragraph 3.3.a.(1) or by proving that historic fitness was previously established as described in Paragraph 3.3.a.(2).

(c) Establishing current fitness.

(d) Establishing an acceptable purpose for presence on the installation, either by means of the credential the individual uses to establish their identity simultaneously establishing an acceptable purpose or by any other means described in Paragraph 3.4.

(2) During the VCP, the procedures will require that:

(a) All acceptable credentials and source identity documents will be visually inspected front and back for signs of alteration or counterfeit, and verified as described in Paragraph 5.3.

(b) Acceptable credentials and source identity documents that appear questionable (e.g., damaged laminates, evidence of tampering) or altered will not be accepted.

(3) The procedures will require that, upon successful completion of the VCP:

(a) Visitors with an enrollable acceptable credential at an ePACS-enabled DoD installation, with or without IMESA functionality, will be enrolled in accordance with Paragraph 4.5 of this issuance.

(b) All other visitors will be issued a pass or credential in accordance with Paragraphs 4.4.c or 4.4.d.

c. Short-Term Visitor Passes. Visitors who successfully complete the VCP with an acceptable purpose and a duration shorter than 8 days, but who are ineligible for enrollment pursuant to Paragraph 4.5, will be issued either a:

(1) Short-term personalized paper or plastic pass. The personalized pass will, at a minimum, list the visitor's name and the dates for which the pass is valid for access. The pass will be valid for the shorter of the visitor's established acceptable purpose, the maximum duration allowed by DoD Component-level policy, or seven days; or

(2) Reusable un-personalized pass. Procedures must be in place to enforce the collection of reusable un-personalized passes as visitors exit to prevent reuse. Any such procedures that entail the collection and holding of personally identifiable information (to include holding credentials) will be compliant with DoDI 5400.11 and Section 552a of Title 5 U.S.C.

d. Long-Term Visitor Credentials. If permitted by DoD Component policy, non-CAC LRC may be issued to individuals who successfully complete the VCP with an acceptable purpose with a duration longer than 7 days and who do not possess an enrollable acceptable credential. These non-CAC LRCs will:

(1) Bear the individual's name, photo, and dates valid.

(2) Be valid for the duration of their established acceptable purpose, the maximum duration allowed by DoD Component policy, or one year, whichever is shorter.

(3) Be enrolled in the local installation ePACS when issued at an ePACS-enabled DoD installation with or without IMESA functionality.

(4) Be enrolled in IMESA when issued at an ePACS-enabled DoD installation with IMESA functionality.

(5) Not be used to circumvent the Tier 1 background investigation and CAC issuance requirements for individuals eligible for a CAC under Volume 1 of DoDM 1000.13.

e. VCP Completion With Redress and Appeal.

(1) An individual who completes the VCP through redress will be handled as any other visitor.

(2) An individual who completes the VCP through appeal will:

(a) Have their enrollment designated as completed through appeal.

(b) Be ineligible for reciprocal acceptance of their enrollment and fitness determination at other DoD installations.

(c) Be ineligible for automatic enrollment in the ePACS of other DoD installations in accordance with Paragraph 4.7.

4.5. ENROLLMENT. All eligible individuals will be enrolled by adding their identity to the local installation ePACS and, at ePACS-enabled DoD installations with IMESA functionality, to IMESA, and linking each individual's identity to the acceptable credential used for enrollment.

a. Eligibility for Enrollment. Enrollment is:

(1) Available to individuals seeking recurring access who successfully complete the VCP and establish their identity by means of an enrollable acceptable credential as listed in Section 5 of this issuance.

(2) Unavailable to individuals who establish their identity using a non-enrollable acceptable credential or any acceptable combination of source identity documents as listed in Section 5, or who fail to complete the VCP.

(3) Unavailable to all individuals at non-ePACS-enabled DoD installations.

(4) Not to be used to circumvent the Tier 1 background investigation and CAC issuance requirements for individuals eligible for a CAC under Volume 1 of DoDM 1000.13.

b. Enrollment Reciprocity. An enrollment conducted at another DoD installation:

(1) Will not be accepted as proof of historic fitness if the enrollment was conducted at an ePACS-enabled installation without IMESA functionality.

(2) Will be accepted as proof of historic fitness if the enrollment was conducted at another ePACS-enabled installation with IMESA functionality within the same DoD Component.

(3) May be accepted as proof of historic fitness if the enrollment was conducted at another ePACS-enabled installation with IMESA functionality within a different DoD Component, subject to DoD Component policy.

c. Enrollment Validity and Expiration. Enrollment will be valid:

(1) At ePACS-enabled DoD installations with IMESA functionality, for 3 years from the date of enrollment in IMESA, until the expiration date on the enrollable acceptable credential used to establish identity, or until 1 year without a visit to a DoD installation, whichever comes first. Upon the expiration of an individual's enrollment in IMESA, the expiration will be propagated to the ePACS at all ePACS-enabled DoD installations with IMESA functionality.

(2) At ePACS-enabled DoD installation without IMESA functionality, for 1 year from the date of enrollment in the local installation ePACS, until the expiration on the enrollable acceptable credential used to establish identity, or until 3 months without a visit to the installation, whichever comes first.

d. Declined Enrollment. An individual who is eligible to enroll but declines or refuses to enroll and subsequently returns to the installation at a later date will be processed as any other unenrolled individual.

4.6. ACCESS CONTROL PROCESS.

a. ePACS-Enabled DoD installations with IMESA Functionality. At ePACS-enabled DoD installations with IMESA functionality, DoD Components will process, directly at the ACP, individuals who have previously enrolled in IMESA and the local installation ePACS and who present the same enrollable acceptable credential that was used to enroll.

(1) If an individual completes the access control process by means of an acceptable credential that does not itself establish purpose, that individual must establish purpose at the ACP before being granted access.

(2) The requirements for gaining unescorted access are fully satisfied.

b. ePACS-Enabled DoD installations without IMESA Functionality. At ePACS-enabled DoD installations without IMESA functionality, DoD Components will process, directly at the ACP, individuals who have previously enrolled in the local installation ePACS and who present the same enrollable acceptable credential that was used to enroll.

(1) Only a CAC, USID, or non-CAC LRC issued by the local installation or region may be used to enroll at ePACS-enabled DoD installations without IMESA functionality. The access control process will only be completed using an acceptable credential that itself establishes purpose. Individuals with other acceptable credentials must be processed through the VCP at the VCC.

(2) The requirements for gaining unescorted access are **partially** satisfied: however, current fitness cannot be established because the local installation ePACS does not interface with IMESA. The residual risk associated with not establishing current fitness must be addressed in the request for ePACS deviation described in Paragraphs 2.4.e, 2.4.f, and 6.2 of this issuance.

c. Non-ePACS-Enabled DoD installations. At non-ePACS-enabled DoD installations, DoD components will process individuals who present a CAC, USID, or non-CAC LRC issued by the local installation or region at the VCC or ACP if permitted by DoD Component and installation-level policies.

(1) The CAC, USID, and non-CAC LRC issued by the local installation or region all establish purpose. The access control process will only be completed using an acceptable credential that itself establishes purpose. Individuals with other acceptable credentials must be processed through the VCP at the VCC.

(2) The requirements for gaining unescorted access are **partially** satisfied: however, current fitness cannot be established because the local installation ePACS does not interface with IMESA. The residual risk associated with not establishing current fitness must be addressed in the request for ePACS deviation described in Paragraphs 2.4.e, 2.4.f, and 6.2 of this issuance.

d. Un-manned Pedestrian ACP. At ePACS-enabled DoD installations with IMESA functionality, DoD Components may implement un-manned (also known as un-attended) ACPs **for pedestrian use only.** ACPs with a single onsite attendant servicing multiple lanes are not considered un-manned ACPs. Un-manned ACPs are subject to the following requirements:

(1) Only a CAC, USID, and non-CAC LRC that has already been enrolled at the installation may be accepted at un-manned ACPs.

(2) Two-factor authentication is required at all times. The second factor may be either personal identification number or biometric, in accordance with DoD Component policy.

(3) The un-manned ACP must:

(a) Be covered by surveillance cameras that are recorded and monitored, either manually or by automated (e.g. motion detection) means, at all times. Recordings will be kept consistent with applicable records schedules and no less than 30 days.

(b) Prevent vehicular access.

(c) Include a mechanism to prevent the entry of more than one person in a single attempt.

(d) Include tamper alarms, monitored at all times, with a response force capable of reaching the un-manned ACP within 15 minutes of alarm.

e. DoD Approval Required for Un-manned Vehicle ACP. DoD Component proposals for un-manned ACPs that allow vehicular access must be submitted to the USD(I&S) for consideration. ACPs with at least one on-site attendant servicing multiple lanes are not considered un-manned.

4.7. AUTOMATIC ENROLLMENT AT THE ACP.

a. At ePACS-enabled DoD installations with IMESA functionality, in lieu of undergoing the VCP at the VCC:

(1) Individuals establishing their identity by means of a CAC, USID, or non-CAC LRC should be automatically enrolled in IMESA and the local installation ePACS by presenting their CAC or USID at the ACP;

(2) Individuals establishing their identity by means of any other enrollable acceptable credential who have previously enrolled in IMESA at another installation should be automatically enrolled in the local installation ePACS by presenting, directly at the ACP, the same acceptable credential used previously for enrollment in IMESA.

b. At ePACS-enabled DoD installations without IMESA functionality, individuals establishing their identity by means of a CAC or USID should be automatically enrolled in the local installation ePACS by presenting their CAC or USID at the ACP in lieu of undergoing the VCP at the VCC.

c. Installations with unique mission requirements may choose not to implement automatic enrollment and instead require individuals who have not previously enrolled at that installation to

be processed through the VCC at their first visit and enrolled for subsequent visits. This is not considered a deviation.

4.8. EPACS FAILURE CONTINGENCIES. DoD Components will establish procedures for ePACS-enabled DoD installations, with and without IMESA functionality, for installation access control in the event of an ePACS failure. Procedures should include visual inspection at the ACP of DoD-issued credentials and processing through the VCP of holders of other credentials; visual inspection of all credentials; and other applicable procedures to account for the specific characteristics of the installation, risk assessments, and DoD Component and installation-level policies.

SECTION 5: ACCEPTABLE FORMS OF IDENTIFICATION

5.1. ACCEPTABLE CREDENTIALS. All credentials must be verified in accordance with the methods defined in Paragraph 5.3. Any time the credential is physically handled it will be visually inspected, front and back, for signs of alteration or counterfeit. Credentials that appear questionable (e.g., damaged laminates, evidence of tampering) or altered will not be accepted for any purpose.

a. Credentials Acceptable at non-ePACS-Enabled DoD installations. Non-ePACS-enabled DoD installations, absent an approved deviation, will accept:

(1) DoD CAC. The CAC simultaneously establishes identity, historic fitness, and purpose.

(2) DoD USID. The USID establishes identity and generally establishes purpose. However, DoD Component and installation-level policy, pursuant to paragraph 3.4.b, may require additional information or documentation to establish an acceptable purpose for access to installations that do not serve benefit populations (such as, but not limited to, retirees and dependents); no deviation is required for such policies.

(3) Non-CAC LRC issued by the **local** installation or region. These credentials simultaneously establish identity, historic fitness, and purpose.

(4) REAL ID-compliant driver's license or non-driver's identification card issued by a State, territory, possession, or the District of Columbia. These credentials establish only identity.

(5) Enhanced driver's license issued by a State, territory, possession, or the District of Columbia. These credentials establish only identity.

(6) U.S. passport or passport card. These credentials establish only identity.

(7) Foreign passport bearing an unexpired immigrant or non-immigrant visa or entry stamp. These credentials establish only identity.

(8) Any other government-issued credential bearing a photograph and deemed acceptable by the DoD Component head and consistent with applicable laws.

b. Credentials Acceptable at ePACS-Enabled DoD installations without IMESA Functionality. ePACS-enabled DoD installations without IMESA functionality, absent an approved deviation, will accept:

(1) DoD CAC. The CAC simultaneously establishes identity, historic fitness, and purpose.

(2) DoD USID. The USID establishes identity and generally establishes purpose. However, DoD Component and installation-level policy, pursuant to paragraph 3.4.b., may require additional information or documentation to establish an acceptable purpose for access to

installations that do not serve benefit populations (such as, but not limited to, retirees and dependents); no deviation is required for such policies.

(3) Non-CAC LRC issued by the **local** installation or region. These credentials simultaneously establish identity, historic fitness, and purpose.

(4) REAL ID-compliant driver's license or non-driver's identification card issued by a State, territory, possession, or the District of Columbia. These credentials establish only identity.

(5) Enhanced driver's license issued by a State, territory, possession, or the District of Columbia. These credentials establish only identity.

(6) U.S. passport or passport card. These credentials establish only identity.

(7) Foreign passport bearing an unexpired immigrant or non-immigrant visa or entry stamp. These credentials establish only identity.

(8) Any other U.S. Federal, State, territory, possession, or District of Columbia Government-issued credential bearing a photograph, including credentials from other paragraphs in this section, deemed acceptable by the DoD Component head and consistent with applicable laws.

c. Credentials Acceptable at ePACS-Enabled DoD installations with IMESA Functionality. ePACS-enabled DoD installations with IMESA functionality, absent an approved deviation, will accept:

(1) The credentials listed in Paragraph 5.1.b of this issuance.

(2) Non-CAC LRC issued by **another** ePACS-enabled installation or region with IMESA functionality. These credentials simultaneously establish identity and historic fitness.

(3) Federal Personal Identity Verification (PIV) card. The PIV simultaneously establishes identity and historic fitness.

(4) Veteran's Health Identification Card (VHIC). The VHIC simultaneously establishes identity and, if the installation has a medical treatment facility, purpose. The VHIC also establishes purpose for individuals accompanying the cardholder.

(5) Non-federal personal identity verification-interoperable (PIV-I) card. The PIV-I establishes only identity.

(6) Transportation Worker Identification Card (TWIC). The TWIC establishes only identity.

(7) Any other U.S. Federal, State, territory, possession, or District of Columbia Government-issued credential bearing a photograph, including credentials from other paragraphs in this section that are deemed acceptable by the DoD Component head and consistent with applicable laws.

d. Summary of Acceptable Credentials. Table 1 contains the acceptable credential information from Paragraphs 5.1.a through 5.1.c in tabular form.

Table 1. Summary of Credential Acceptability, Enrollability, and Requirements Established

Acceptable Credential	non-ePACS-enabled		ePACS-enabled without IMESA		ePACS-enabled with IMESA		If Acceptable, Establishes:		
	Acceptable	Enrollable	Acceptable	Enrollable	Acceptable	Enrollable	Identity	Historic Fitness	Purpose
CAC	X		X	X	X	X	X	X	X
USID	X		X	X	X	X	X		X[2]
Non-CAC Local or Regional DoD Credential issued by the **local** installation or region	X		X	X	X	X	X	X	X
Non-CAC Local or Regional DoD Credential issued by **another** installation or region					X	X	X	X	
REAL ID-compliant driver's license, enhanced driver's license, or non-driver's identification card issued by a State, territory, possession, or the District of Columbia	X		X		X	X	X		
U.S. or Foreign Passport or Passport Card	X		X		X		X		
TWIC					X	X	X		
VHIC					X	X	X		X[1]
Federal PIV					X	X	X	X	
Non-Federal PIV-I					X	X	X		

[1] The VHIC establishes purpose only at installations that have a medical treatment facility, and establishes purpose both for the cardholder and for the cardholder's accompanying caregiver.

[2] The USID generally establishes purpose, but may be deemed as not establishing purpose at more-restricted installations that do not serve retirees or dependents.

5.2. SOURCE IDENTITY DOCUMENTS. All source identity documents must be visually inspected for known security features, as applicable, and for signs of alteration or counterfeit. Electronic verification is not required for source identity documents, but may be performed if it is available. Unless otherwise specified in this section, source identity documents establish only identity.

a. Combinations Accepted at all Installations. DoD Components will accept the following combinations of source identity documents at all types of DoD installations:

(1) TWIC used in conjunction with a driver's license issued by a State, territory, possession, or the District of Columbia that is not REAL ID-compliant bearing the same name and similar photograph. In this situation:

(a) The TWIC is the credential used to establish identity for the purpose of access control.

(b) The non-REAL ID-compliant driver's license is used to establish identity for the purpose of force protection.

(2) VHIC used in conjunction with a driver's license issued by a State, territory, possession, or the District of Columbia that is not REAL ID-compliant bearing the same name and similar photograph. In this situation:

(a) The VHIC is the credential used to establish identity for the purpose of access control.

(b) The non-REAL ID-compliant driver's license is used to establish identity for the purpose of force protection.

(3) Original or certified true copy of a birth certificate bearing a raised seal, social security card, and driver's license issued by a State, territory, possession, or the District of Columbia that is not REAL ID-compliant. All three documents must bear the same name or a former name as documented on acceptable name change documentation such as a court order, marriage certificate, or divorce decree. In this situation:

(a) The birth certificate and social security card are used to establish identity for the purpose of access control.

(b) The non-REAL ID-compliant driver's license is used to establish identity for the purpose of force protection.

b. Component-defined Combinations. DoD Component policy will establish other acceptable source identity documents, and the combinations in which they will be accepted. The combinations of source identity documents must reasonably approximate the rigor associated with obtaining a State or Federal photo ID, and provide a reasonable assurance in the identity established.

5.3. VERIFICATION OF CREDENTIALS. All credentials will be verified in accordance with Tables 2 and 3 based on the credential being used, the type of installation, and whether verification is taking place during the VCP (that is, at the VCC during enrollment) or during the access control process (that is, at the gate at time of access).

a. PIV and PIV-I Credentials. Public key infrastructure verifications of Federal PIV credentials and Non-Federal PIV-I credentials will be in accordance with National Institute for Standards and Technology (NIST) Federal Information Processing Standard 201-2, NIST Special Publication (SP) 800-116, NIST SP 800-73-4, and NIST SP 800-96, and may be performed directly or via the IoLS.

b. TWIC Credentials. Public key infrastructure verifications of TWIC credentials will be in accordance with Section 101 of Title 33, Code of Federal Regulations, and may be performed directly or via the IOLS.

Table 2. Verification Method by Credential and Type of Installation

Credential	During the Visitor Control Process (i.e., at the VCC for enrollment)			During the Access Control Process (i.e., at the ACP for access each time)		
	Non-ePACS-enabled	ePACS-enabled without IMESA	ePACS-enabled with IMESA	Non-ePACS-enabled	ePACS-enabled without IMESA	ePACS-enabled with IMESA
CAC	A	A	B2	A	B1 or E1*	B2 or E2*
USID	A	A	B2	A	B1	B2
Non-CAC Local or Regional DoD Credential	A	A	B2	A	B1	B1
REAL ID-compliant driver's license, enhanced driver's license, or non-driver's identification card	A	A	A			B1
U.S. or Foreign Passport or Passport Card	A	A	A			
TWIC			D			C or E
VHIC			B1			B1
Federal PIV			D			C or E
Non-Federal PIV-I			D			C or E

* If intermittently required due to throughput, traffic, or other circumstances, U.S. citizen CACs (indicated by a white or green stripe) may be primarily verified visually, with electronic verification performed on a random sampling of CACs. Non-U.S. citizen CACs (indicated by a blue stripe) **must** be scanned at ACPs.

Blank cells indicate that credential is not acceptable in that situation.

Table 3. Verification Methods

Method	Verify the Credential	Verify the Cardholder
A (high risk)	Visually.	By comparing the individual presenting the credential with the photo printed on the card.
B1 (medium risk)	By reading an identifier from a barcode and verifying that identifier against a local authoritative system capable of tracking revocations at the installation level, such as the local ePACS.	By comparing the individual presenting the credential with the photo stored in an authoritative system, such as the local ePACS or Defense Enrollment Eligibility Reporting System (DEERS).
B2 (low risk)	By reading an identifier from a barcode and verifying that identifier against an interconnected authoritative system capable of tracking revocations at the enterprise level, such as DEERS.	By comparing the individual presenting the credential with the photo stored in an authoritative system, such as the local ePACS or DEERS.
C (low risk)	By performing a full public key infrastructure authentication against either the Card Authentication function or the PIV Authentication function, including verifying including the signature, trust chain, expiration dates, policy under which it was issued, and continued validity of the certificate against a certificate revocation list or Open Certificate Status Protocol responder.	By comparing the individual presenting the credential with the photo stored in an authoritative system, such as the local ePACS or DEERS.
D (low risk)	By performing a full public key infrastructure authentication against either the Card Authentication function or the PIV Authentication function, including verifying including the signature, trust chain, expiration dates, policy under which it was issued, and continued validity of the certificate against a certificate revocation list or Open Certificate Status Protocol responder.	By using a credential verification process that requires card activation (such as PIV Authentication); comparing the individual presenting the credential against the signed digital photo stored on the card provided the signature on the digital photo is verified; or comparing the individual against the signed biometric object stored on the card provided the signature on the biometric object is verified.
E1 (medium risk)	By reading an identifier such as the Card Holder Unique Identifier or Globally Unique Identifier, and verifying that identifier against a local authoritative system capable of tracking revocations at the installation level, such as the local ePACS.	By comparing the individual presenting the credential with the photo stored in an authoritative system, such as the local ePACS or DEERS.
E2 (low risk)	By reading an identifier such as the Card Holder Unique Identifier or Globally Unique Identifier and verifying that identifier against an interconnected authoritative system capable of tracking revocations at the enterprise level, such as the Federal Bridge.	By comparing the individual presenting the credential with the photo stored in an authoritative system, such as the local ePACS or DEERS.

SECTION 6: IMPLEMENTATION

6.1. COMPONENT IMPLEMENTING POLICIES. The implementing policies issued by DoD Component heads will include, at a minimum:

a. Fitness criteria for unescorted access in accordance with Paragraph 3.3, until a DoD standard for fitness is defined.

b. Source identity documents (and their acceptable combinations) and any other acceptable credentials which may be used to establish identity in accordance with Paragraph 3.2 and Section 5.

c. Any additional means which may be used to establish historic fitness or U.S. citizenship, both in accordance with Paragraph 3.3.

d. Procedures and parameters for applying this issuance to installations with large unoccupied, undeveloped space in accordance with Paragraph 3.1.

e. Permissibility and criteria for acceptance of inter-component enrollments.

f. Acceptable purposes for presence on the installation in accordance with Paragraphs 3.4 and 6.3.

g. Procedures and requirements for handling special events and emergencies in accordance with Paragraph 3.5.

h. Permissibility of trusted traveler programs, and any other criteria, in addition to U.S. citizenship and DoD affiliation, used to authorize individuals to vouch for individuals seeking trusted traveler access, and under which parameters such access will be permitted in accordance with Paragraph 4.2.

i. ePACS failure contingency plans.

j. Escort parameters, including but not limited to classes of individuals permitted to escort, training required to escort (initial and recurring), and number of visitors per escort.

k. Specific procedures for processing visitors, also known as the VCP, that meet the requirements in Section 3.

l. Specific procedures for controlling access, also known as the access control process, that meet the requirements in Section 3 and Paragraph 4.6.

m. The maximum permitted duration for short-term visitor passes and the permissibility of and maximum permitted duration of long-term visitor passes, in accordance with Paragraph 4.4.

n. The requirements for gaining escorted access, and procedures for handling visitors who do not meet the requirements for unescorted access.

o. Variances from DoD Component-level policy available to installation commanders in Paragraphs 6.1.f through 6.1.n of this issuance. Variances from DoD Component-level policy are not permitted for Paragraphs 6.1.a through 6.1.e.

6.2. ALLOWABLE DEVIATIONS. When approved in accordance with Paragraph 2.4.e and 2.4.f, deviations may only include:

a. Absence of an ePACS or use of an ePACS that is not compliant with Paragraph 2.4.c.(1) due to unique mission as deemed by the DoD Component head (including a mission that requires the installation to be open to the public).

b. Precluding the use of one or more of the credentials listed in Section 5 as acceptable for their type of installation due to unique mission requirements in accordance with Paragraph 3.2.

c. More restrictive access control requirements in accordance with Paragraph 3.7.

6.3. COMPONENT POLICY FOR ACCEPTABLE PURPOSES. DoD Component-level policy will determine whether the following are acceptable purposes for access to DoD Component installations (this list is not exhaustive and only includes certain circumstances that are to be expressly addressed in DoD Component policy.)

a. An employee, contractor, or volunteer of the American Red Cross providing a service on the installation that has been requested by the installation commander.

b. An employee, contractor, or volunteer of the United Services Organization, Incorporated providing a service on the installation that has been requested by the installation commander.

c. A driver for a transportation network company or other personnel transportation company picking up or a dropping off a passenger from or to a barracks, housing, lodging, hospital, or community area. Both the driver and passenger must be granted unescorted access to the installation, in accordance with Section 3 of this issuance. In these situations:

(1) The driver's acceptable purpose is providing transportation to the passenger. The driver's access shall be temporary and limited in scope and time to what is necessary to fulfill this acceptable purpose.

(2) The passenger must have their own acceptable purpose in accordance with Paragraph 3.4 of this issuance.

GLOSSARY

G.1. ACRONYMS.

ACP	access control point
CAC	common access card
DEERS	Defense Enrollment Eligibility Reporting System
DIA	Defense Intelligence Agency
DoDD	DoD directive
DoDI	DoD instruction
DoDM	DoD manual
ePACS	electronic physical access control system
IMESA	Identity Matching Engine for Security and Analysis
IoLS	Interoperability Layer Service
NCIC	National Crime Information Center
NIST	National Institute for Standards and Technology
PIV	federal Personal Identity Verification
PIV-I	non-federal Personal Identity Verification – Interoperable
SP	special publication
TWIC	Transportation Worker Identification Card
U.S.C.	United States Code
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USID	Uniformed Services Identification card
VHIC	Veteran Health Identification Card
VCC	visitor control center
VCP	visitor control process

G.2. DEFINITIONS. Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

acceptable credential. A credential that, depending on the type of installation, must be accepted as proof of identity, historic fitness, or purpose, in accordance with Section 5.1.

ACP. Identified gap in an installation's perimeter security for pedestrian and/or vehicular access. Often called an entry control point or simply "gate." Includes commercial vehicle inspection points.

appeal. A process for an individual with accurately identified derogatory information that prevents individuals from establishing either historic or current fitness to seek an exception due to their specific circumstances, allowing them to be granted unescorted access.

automatic enrollment. A process by which certain individuals may be enrolled in an installation ePACS and, if the installation has IMESA functionality, in IMESA, without undergoing the VCP or being processed at the VCC.

credential. A form of identification that, on its own, associates a specific person with their specific identity, biographic, and, in some cases, biometric information. For example, a driver's license. A document that contains identity information but cannot be associated with a specific person (for example, if it has no photograph or biometric information) is not a credential, but may be a source identity document.

current fitness. A determination that an individual has no pending criminal cases or actions against him or her and is not listed on any U.S. Government terrorism lists that would indicate that such individual may pose a risk to the safety, security, and efficiency of the installation or its occupants.

deviation. A divergence from a requirement or procedure that is not intended to be temporary or corrected.

derogatory information. Information that reflects on the integrity or character of an individual that indicates that such an individual may pose a risk to the good order, discipline, morale, or safety of a DoD installation or the resources or personnel on that installation. Examples include, but are not limited to, aspects of an individual's criminal history or current status as wanted or as a known or appropriately suspected terrorist.

DoD affiliation. The status of being officially attached or connected to DoD by means of employment (either as a DoD civilian or military), contract (as a DoD contractor or sub-contractor), government support agreements pursuant to DoDI 4000.19, or statutorily provided benefit (as a military retiree or dependent).

electronically verify. The process of confirming, by cryptographic means or querying the original issuer, that a presented credential is authentic (not counterfeit) and still valid (not revoked, cancelled, or otherwise reported lost, stolen, or compromised).

enrollment. A process that allows individuals who anticipate a subsequent visit to the installation to persist their established fitness, but not purpose, facilitating future entry.

enrollment reciprocity. The acceptance of an enrollment conducted at another DoD installation as proof of an individual's established fitness, but not purpose.

enrollable credential. A type of credential that includes a machine-readable identifier that can be scanned, understood, and processed by an ePACS.

ePACS. An information technology system that provides a "grant" or "deny" decision or recommendation based on a presented identification card, optional additional authentication factors such as a PIN or biometric input, an identity database, and one or more business rules that determines which individuals are authorized access.

escorted access. A type of access where an individual must be appropriately accompanied at all times to ensure that the escorted individual does not cause unacceptable risk to the safety, security, or efficiency of an installation or its occupants.

fitness. A determination based on historic and current information that an individual is likely not a risk to the safety, security, and efficiency of an installation or its occupants.

historic fitness. A determination that an individual's criminal history reflects a level of character and personal conduct that does not pose a risk to the safety, security, and efficiency of an installation or its occupants.

limited access control requirements. Situations where physical access is either limited to small numbers of individuals who are generally known to each other, or to rare and occasional periods. For example: a location with ten assigned employees and infrequent visitors, or a radio transmission tower that operates unmanned except for monthly maintenance periods.

installation. The grounds of, but not buildings on, a base, camp, post, station, yard, center, homeport facility for any ship, or other activity under DoD jurisdiction, including any leased facility, that is located within any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, or Guam that have a perimeter barrier (such as a fenceline or wall), one or more access control points (sometimes called entry control points), and a method for processing visitors. Such term does not include any facility used primarily for civil works, rivers and harbors projects, or flood control projects.

personnel transportation company. An entity that provides transportation of individuals, rather than of material, as a for-hire service. Examples include but are not limited to taxi cabs, limousine services, and bus companies.

purpose. An individual's reason for seeking access to an installation.

source identity document. A document that establishes that specific identity exists, though it does not associate that identity with a specific person. For example, a birth certificate or social security card. These documents may be used in conjunction with others to associate a specific person with a specific identity.

redress. A process for an individual to deconflict his or her identity with that of another individual with whom they are frequently or easily mistaken (such as two individuals with similar names or similar identifiers, one with a criminal history and one without). Redress can be accomplished by providing additional biographic information to distinguish between the identities (such as a date of birth or social security number) or biometric information (such as fingerprints). Redress allows the proper identity to be evaluated for fitness.

special event. Planned time-bound activities (either one-time or recurring) that by their nature have a number of non-installation-assigned individuals attending, and are often characterized by a desire for mass public participation by individuals not otherwise eligible for recurring access to the installation. Examples include, but are not limited to, graduations, sporting events such as military academy football games, conferences, and public exhibitions.

temporary waiver. A suspension, for a short, well-defined time period, of a requirement or procedure with the intention of reinstating it at the end of that time period.

transportation network company. An entity outside of the Department of Defense that provides a commercial transportation service to a rider, including a company that uses a digital network to connect riders to drivers for the purpose of providing transportation.

trusted traveler access. A type of access where an individual is granted entry to the installation based on another authorized person's verification of their identity, fitness, and purpose.

unescorted access. A type of access where an individual is able to travel unaccompanied on an installation

USID. Sometimes called the TESLIN or the Dependent or Retiree ID Card. Includes the DD Form 2 (Retired, Reserve, and Reserve Retired versions), DD Form 1173 and 1173-1, DD Form 2765, and the DoD Civilian Retiree Card as described by DoDI 1000.13 and Volumes 1 and 2 of DoDM 1000.13.

REFERENCES

Code of Federal Regulation, Title 33

DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence and Security (USD(I&S))," October 24, 2014, as amended

DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense," January 7, 1980

DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019

DoD Instruction 1000.13, "Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals," January 23, 2014, as amended

DoD Instruction O-2000.16, Volume 1, "DoD Antiterrorism (AT) Program Implementation: DoD AT Standards, November 17, 2016, as amended

DoD Instruction O-2000.16, Volume 2, "DoD Antiterrorism (AT) Program Implementation: DoD Force Protection Condition (FPCON) System, November 17, 2016, as amended

DoD Instruction 4000.19, "Support Agreements," April 25, 2013, as amended

DoD Instruction 5200.08, "Security of DoD Installations and Resources and the DoD Physical Security Review Board," December 10, 2005, as amended

DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015, as amended

DoD Instruction 5505.17, "Collection, Maintenance, Use, and Dissemination of Personally Identifiable Information and Law Enforcement Information by DoD Law Enforcement Activities," December 19, 2012, as amended

DoD Instruction 8910.01, "Information Collection and Reporting," May 19, 2014, as amended

DoD Manual 1000.13, Volume 1, "DoD Identification (ID) Cards: Identification (ID) Card Life-Cycle," January 23, 2014, as amended

DoD Manual 1000.13, Volume 2, "DoD Identification (ID) Cards: Benefits for Members of the Uniformed Services, Their Dependents and Other Eligible Individuals," January 23, 2014, as amended

DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information," February 24, 2012, as amended

Federal Information Processing Standard 201-2, "Personal Identity Verification of Employees and Contractors," August 2013

Memorandum of Understanding between the Federal Bureau of Investigation and the Department of Defense, Annex D, "Terrorist Screening Information Sharing," February 22, 2012

National Institute of Standards and Technology Special Publication 800-73-4, "Interfaces for Personal Identity Verification," May 2015

National Institute of Standards and Technology Special Publication 800-96, "PIV Card to Reader Interoperability Guidelines," September 2006

National Institute of Standards and Technology Special Publication 800-116, "A Recommendation for the use of PIV Credentials in Physical Access Control Systems," November 2008

Public Law 109-13, Title II, "Improved Security for Drivers' Licenses and Personal Identification Cards," May 11, 2005 (also known as "the REAL ID Act of 2005")

Public Law 110-181, Section 1069, "National Defense Authorization Act for Fiscal Year 2008," January 28, 2008

Public Law 114-92, Section 1086, "National Defense Authorization Act for Fiscal Year 2016," November 25, 2015

Public Law 116-92, "National Defense Authorization Act for Fiscal Year 2020," December 20, 2019

United States Code, Title 5, Section 552a (also known as "the Privacy Act")

United States Code, Title 44, Chapter 35, Subchapter I (also known as "the Paperwork Reduction Act")